



ACCESS CONTROL STANDARD

Standard #: S131

Version #: 2.0

Date: September 2024

Technology Services Division

Technology Services Standards

Ownership/Stewardship

Domain	Owner	Steward
Security and Privacy	Deputy Chief Technology Officer, Technology Service Delivery	Infrastructure Service Delivery Director

Approval

Section	Name	Approval Date
Enterprise Architecture Review Board	Andrew Berenyi, Andrew Chan, Bonita See, Florian Puthod, Gohar Khera, Hemali Wijesundara, Jessica Chi, Johan Macedo, Julie Attard, Karthik Santosh, Lenny De Marco, Marco Palermo, Mladen Subara, Nigel Arjoonsingh, Richard Liu, Rob Bezaire, Robert Ambra, Tim Kung, Victor Chan	September 10, 2024

Approval History

Version #	Approval Date	Approved By	Approved with comments	Next Review
0.11	Aug 2019	Lawrence Eta, CIO (Acting)		08/2020
0.12	Dec 2019	Amended	Password parameters modify to reflect industry specifications, full review required by next review date.	08/2020

Contact Information

Marco Narduzzo
Standards Officer (Standards)
Marco.Narduzzo@toronto.ca
Business Solutions, Architecture & Standardization
Technology Services Division
Technology Services Division
Business Solutions Architecture & Standardization

Table of Contents

Technology Services Standards.....	1
Ownership/Stewardship	1
Approval	1
Approval History	1
Contact Information.....	1
1. Purpose.....	4
2. Application	4
3. Definitions.....	4
4. Standard	7
4.1 Account Management.....	7
4.1.1 Account Types	7
4.1.2 Account Lifecycle Management	9
4.1.3 Role Management.....	13
4.2 Password Rules	14
4.2.1 Password / Phrase Settings	14
4.3 Access Control Classification Framework	15
4.4 Wireless Access.....	20
4.5 Remote Access	20
4.6 System Access Control	21
4.6.1 System Use Notification	21
4.6.2 Session Control	22
4.6.3 Logging and Monitoring.....	22
4.7 Use of Information Systems by External Party	22
4.8 Use of Third-Party Systems.....	23
4.9 Use of Cloud Services	23
4.10.1 Protecting Passwords.....	24
4.10.2 Use of Access.....	24
4.10.3 Administrator Account Usage	25
5. Standard Approval and Review Schedule.....	25
6. Related Documents	26
7. Contact.....	26

APPENDIX A:	27
Roles & Responsibilities Matrix by Account Type.....	27
Legend:	27
Administrator Account	27
Regular User Account	28
Service Account.....	28
Generic User Account	29
Public Account	29
Role Management.....	31

1. Purpose

This document defines the standards governing the City of Toronto's information technology infrastructure in a manner that protects the integrity and availability of the City's resources.

Standards are developed and maintained to achieve a collaborative approach that ensures City software, hardware, and data systems all function smoothly together in a secure environment, while gaining efficiencies and cost savings through

- the use of compatible systems and the consistent use of technology.
- consistent staff training and transferable skills set among employees.
- volume-discount purchasing.
- minimized support costs.
- improved communication and technical transference across the City.
- fit with current technology and future advancements.

This document is for protecting the informational assets within the City of Toronto computing environment.

2. Application

Corporate Technology standards apply to all individuals using technology provided by the City or authorized to access the City of Toronto infrastructure and technology assets to fulfill their duties and the City's business goals. All City technology assets are subject to these standards, regardless of their use or physical location.

3. Definitions

1. **ACCESS MANAGER (PROCESS OWNER) (ITIL)** – grants authorized users the right to use a service, while preventing access to non-authorized users. The Access Manager essentially executes policies defined in Information Security Management.
2. **ACCESS RIGHTS** – are a set of data defining what services a user is allowed to access. This definition is achieved by assigning the user, identified by their User Identity, to one or more user roles.
3. **ACCOUNT APPROVER** – is the individual with the authority to accept and reject account access request.
4. **ACCOUNT OWNER** – is the individual who has been assigned the account. Credentials are associated to the account holder's identity.
5. **ACCOUNT OWNER MANAGER** – is within the organizational structure, the person to whom the Account Owner reports.
6. **AUTHENTICATION** - is verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

7. **AUTHORIZED USERS** – are all individuals who have been granted access to the City's Information Technology Assets. This includes, but is not limited to, employees, consultants, contractors, subcontractors, individuals on secondment to the City, students and volunteers at the City of Toronto and Accountability Officers and anyone working or volunteering for or in their Offices subject to Section 3-10 F(5), Chapter 3, Accountability Officers, of the Toronto Municipal Code.
8. **AVAILABILITY** – is defined as ensuring timely and reliable access to and use of information by authorized users and systems. A loss of availability is the disruption of access to or use of information or an information system.
9. **CONFIDENTIALITY** – is defined as preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and property information. A loss of confidentiality is the unauthorized disclosure of information.
10. **CREDENTIAL ISSUER** – is the individual that issues the authentication credentials to the account owner or disables authentication credentials.
11. **DISABLEMENT** – Deprovisioning accounts due to but not limited to termination, retirement, and lay off, long term leave, maternity, and paternity leave.
12. **EXTERNAL PARTY** – is an individual or organization that is a legal entity.
13. **INTEGRITY** – is defined as guarding against improper addition, modification, or destruction of information. Enforcing integrity to preserve the timeliness, accuracy, and completeness of information.
14. **LOCAL ADMINISTRATOR ACCOUNT** – is the built in local system account generally used to perform Local Administrative tasks on computers before connecting to the City domain, to image or to troubleshoot network connectivity.
15. **MAY** – means the item is an optional requirement.
16. **MULTI-FACTOR AUTHENTICATION** - is a security enhancement that requires someone to present two or more pieces of evidence – one's credentials – when logging in to an account. Credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Credentials must come from two distinct categories to enhance security – so entering two different passwords would not be considered multi-factor.
17. **MUST** – means an absolute requirement of the specification. See also "SHALL."
18. **PRINCIPLE OF LEAST PRIVILEGE** - is allowing only authorized accesses for users (or processes acting on behalf of users) that are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
19. **ROLE MANAGER** – the individual that is knowledgeable about which person should be assigned which role within a system.

- 20. **SEGREGATION OF DUTY** - addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Segregation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.
- 21. **SHALL** – means an absolute requirement of the specification. See "MUST"
- 22. **SINGLE-FACTOR AUTHENTICATION** - is a security enhancement that requires someone to present one authentication factor (something the user knows or something the user has or something the user does) to authenticate an individual's identity.
- 23. **SHOULD** – means there may be valid reasons in particular circumstances to ignore a particular item, but the full implication must be understood and carefully considered before choosing a different course.
- 24. **SPONSOR** – means a City of Toronto Manager responsible for an external party.
- 25. **SYSTEM ADMINISTRATOR** – implements changes to the access control system.
- 26. **THIRD PARTY SYSTEM** – a software/hardware component developed to be distributed or sold by an entity other than the original vendor of the development platform.

4. Standard

4.1 Account Management

The discipline of Account Management addresses requesting, establishing, issuing, suspending, modifying, and closing user accounts and related user access rights by following a set of user account management procedures.

4.1.1 Account Types

Any account created and maintained by the City of Toronto must be classified as one of the following:

ACCOUNT TYPE	ACCOUNT DESCRIPTION	EXAMPLES
Administrator Account	An account that has administrative or high privileges such as management of a computing system, services and/or application resource. Examples would be an “Elevated Privilege” account or a Local Administrator account.	Enabling services, modifying access and permissions.
Regular User*	An account that is used by a City of Toronto user (staff or non-staff member) to access and operate City of Toronto systems. Such account is usually defined and is a part of the City of Toronto directory services.	Typical employee or contractor account that allows access to workstation.
Service Account (Resource Account)	An account that is usually created to allow services and/or applications to interact with the operating system without user interface.	Backend connection to a remote service.
Generic or Shared User Account	An account that is used by multiple City of Toronto users.	Training purposes, shared workstation.
Public Account	An account that is for users that are not acting on behalf of the City of Toronto, usually for public applications and/or services. Public Accounts may be managed outside the City of Toronto directory services (e.g., local account repository managed by the application).	Account created by business owner to use the Municipal Licensing Services web application or a resident using My Toronto Pay.
Cloud-Only Account	An account that is created and managed solely within City of Toronto Cloud environment to perform administration task and/or interact with operation system/API for user authentication.	Cloud only privileged account, Cloud only Application account. Azure Global Admin account and managed identity to access Azure Key Vault.

Cloud Collaboration Guest Account	An external account that is created or invited to City of Toronto Cloud environment (for example Azure/O365/AWS/etc.) for cloud resource collaboration.	Guest user from third-party partner provisioned to City's SharePoint Online Site for collaboration.
Vendor Support Account	A user account that allows a vendor to gain access to the City's IT infrastructure to provide services.	Bell UC support account.
Vendor Supplied Account	The accounts that were configured by the vendor as part of the factory settings and may be used for device installation.	(For example, "Administrator" in Windows, "root" in Unix/Linux).

Table 1 Account Type & Description

*An account that has not been classified but has access to the City of Toronto internal network, will be defined and set as "Regular User" by default.

4.1.2 Account Lifecycle Management

4.1.2.1 Provisioning

Before creating and enabling an account, an account owner must be identified. The owner will acknowledge the ownership of the new account and will be the "point of contact" for future account related inquiries. The person associated with the user ID is the account owner. For service account and generic accounts, though there is no person directly associated with the account, there still must be a City of Toronto staff who is identified as the person responsible for the secure maintenance of the account. For Cloud Guest Accounts, a City of Toronto staff must be identified to govern and maintain proper access for the account.

4.1.2.1.1 ID Creation

When provisioned: User IDs shall:

1. Be unique within the City of Toronto environment.

With the exception of service and generic accounts:

2. Not contain information related to job function, location, or job status. Any information related to organization or functions should be linked and not contained in the format of the ID.
3. Not be reused and assigned to a different person or system.
4. New IDs shall be issued when there are significant role changes.

5. Be set to automatically expire or become disabled at the end of the contract for third party staff (contractors, consultants, outsourcing suppliers, etc.). Care must be taken to change this date if the contract is renewed. A review of these IDs by the contracting owner/Business Unit shall be undertaken at least annually to verify their continued need.

4.1.2.1.2 Process Controls

Separation of duty must be enforced such that the account requester, account approver, and credential issuer are separate people.

All access requests and their approval must be documented and stored in accordance with the City of Toronto's records management standards. These include:

- a. [Information Management Accountability Policy](#)
- b. [Responsible Record Keeping Directive and Guideline](#)
- c. [Duty to Document Fact Sheet](#)

Such records must be stored in a central repository such that any record can be efficiently and effectively located.

If the account owner must manage their own password:

1. Temporary authentication information must initially be provided. The maximum length of time in which temporary authentication information will remain valid if the user has not used the account is based on the "Mapping of Access Control to Data Sensitivity Classification" section of this standard. Once the maximum length of time (from the time the credential is issued) has been reached and the user has not applied the temporary credential to the applicable system, the temporary credentials must expire, and the user must reapply for authentication credentials.
2. The account owner is forced to create or change their password upon the first use of the system.
3. The system must ensure that the changed password is different from the temporary password.
4. The password complexity of the temporary password must follow the password complexity requirement of this standard.
5. Any temporary passwords must be sent to the account owner in a manner that protects confidentiality of the authentication credentials (see Mapping of Access Control to Data Sensitivity Classification)
6. Acknowledgement of the successful receipt of the temporary password must be received by the credential issuer.
7. Each temporary password must be unique.

The account owner must be notified of any changes to their account credentials.

4.1.2.1.3 Service and Generic Account

Each Service and Generic User account can only be valid on a predefined system or set of systems. The creation of a Generic User account requires a risk assessment by the Office of the CISO and subsequent risk acceptance by the account owner before approval by the Office of the CISO (see link to Access Management Policy section 4.1.3). Creation of a Service Account requires a self-attestation of compliance with the Credential Management Policy (section 4.1.7).

It is the responsibility of the account owner or requester to use the account, in compliance with access management policies and standards.

4.1.2.2 Access Control Review

There are two types of access control reviews:

- a) Periodic Review: A process to review all accounts assigned to both information system and applications/services must be engaged based on the “Mapping of Access Control to Data Sensitivity Classification” section of this standard.
- b) Individual Review: A review of an individual’s accounts must be conducted when the business responsibilities of the individual changes.

Access control reviews must be conducted periodically on all accounts. (See “Minimum Access Control Requirements Mapped to Various Elements of Access Control” matrix for frequency of review) In addition, individual reviews must be conducted when individual responsibilities change.

Access control reviews must be conducted by the Role Manager and signed off by the Access Manager. The reviewer (Role Manager) must:

- (i) Validate the continued business need for each active account with the resource owner.
- (ii) Ensure that application/service account credentials will be disabled when no longer needed.
- (iii) Reconcile existing accounts with account access requests, modification requests, and disablement requests.
- (iv) Note and initiate the revocation immediately of any access not documented or approved by the account provisioning process.
- (v) Access rights assigned to accounts must be reviewed and validated to ensure that the principle of least privilege is enforced.
- (vi) Include a review of access rights related updates to identify suspicious activities, with special emphasis on administrative-level privilege that may signal compromised accounts. Examples of suspicious activities include:
 - a) Unauthorized changes to existing administrative accounts and privileges.
 - b) Creation of new administrative accounts/groups without approval or documentation.

4.1.2.3 De-Provisioning or Responsibility Change

In case of a user changing roles or leaving the organization, the Account Owner Manager must immediately:

1. Notify the Systems Administrator via the IT Service Desk, IT Self Service, or other methods as appropriate of:
 - a. The account to be disabled (e.g., network accounts).
 - b. Who the new owners are of the remaining active accounts (e.g., Service Accounts).
 - c. Any access rights assigned to the Account Owner that must be changed due to the account owner's change in business responsibilities (e.g., leaving the organization, change of role, decommission of a system) so that the principle of least privilege is maintained.
2. Inform account administrators of all third-party providers to the City of Toronto in which the user had an account, of the user's departure, so any user's accounts on the third-party systems are disabled.

4.1.2.3.1 Process Controls

Segregation of duty must be enforced such that the account owner, access manager (account change approver), and the system administrator who manages the credentials or access rights are separate people.

All privilege modification or account disable requests and their approval must be documented and stored in accordance with the City of Toronto's records management standards.

Unless notified otherwise, the user's manager will automatically become the active account owner.

Upon notification, accounts that are no longer needed must be disabled immediately.

Disabled accounts must never be re-provisioned (i.e., not repurposed for other users). If the user leaves the employment of the City and then returns, a new User ID must be issued unless they are returning to the same Division or granted approval by their previous Division. User IDs may also be reused in the following limited circumstances such as: employees returning to the same Division from leaves, acting assignments, and other temporary assignments.

4.1.2.4 Authentication

The confidentiality and integrity level of the information accessed will determine the level and type of authentication (whether single or multifactor authentication is required). See "[Mapping of Access Control to Data Sensitivity Classification](#)" Section 4.3 Table 3 in this standard. If multifactor authentication is used, all factors must be bound to the same identity and the binding is enforced at the time of authentication.

Passwordless (“strong authentication”) tokens may be used as one of the factors in a single or multifactor authentication. The system must enforce that when a maximum number of consecutive failed authentication attempts is reached (e.g., wrong password), access must be temporarily denied for at least 15 minutes (locked account) or until an administrator enables the user ID after successfully validating the user’s identity. (See “Minimum Access Control Requirements Mapped to Various Elements of Access Control” matrix for what the maximum number of attempts should be and when positive user identification is required before authentication credentials are reset).

Failed authentication attempts should be considered consecutive even if performed from different systems and/or with a considerable time gap.

4.1.2.5 Authorization

In cases where a person may perform several roles within a system, the User ID shall be allocated the required level of access rights to effectively conduct these roles. Before a person may perform several business roles, the business process owner, must ensure that the principle of segregation of duty remains in enforcement or compensating controls are added if segregation of duty cannot be enforced.

4.1.3 Role Management

When possible, access rights and controls must be assigned to roles (or groups representing the role) and not to specific user accounts.

Each role/group must be assigned:

- a) An owner.
- b) The minimum access rights required for business purposes. Provisioning of access rights must be based on the principle of least privilege and must enforce separation-of-duty and need-to-know.

A process to review the role/group permissions and user accounts must be conducted by the group’s owner to identify as defined in section 4.7.3 Account Recertification of the Access Management Policy and Section 4.3 [Mapping of Access Control to Data Sensitivity Classification](#) below:

- (i) Unnecessary access rights to be removed as soon as possible.
- (ii) Accounts that are disabled or no longer associated with the specific role to be removed from the group as soon as possible.

4.1.4 Privileged Access Management

Accounts with privilege access in a system should be utilized, accessed, and managed via a privilege access management service when available and applicable.

4.2 Password Rules

Any set of credentials within the City of Toronto environment must include, at minimum, a User ID, and a password. All employees who are authorized to access city resources are responsible for creating and choosing strong passwords.

4.2.1 Password / Phrase Settings

Passwords that are created and assigned to any account within the City of Toronto environment must meet the following criteria. Password authentication systems must be able to enforce the following criteria:

#	Setting	Local Administrator Account	Administrator Account (other than Local Administrator Account)	Service Account	All Other Accounts	Cloud Only Account
1	Minimum Character Length	16	12	32	12	8
2	Maximum Lifetime (Expiry) in Days	365	60	365	90	90
3	Minimum Lifetime in Days	0	0	0	0	0
4	Meet Complexity Requirements (at least 1 non-alphanumeric or 1 alphanumeric, uppercase, 1 lowercase)	Yes	Yes	Yes	Yes	Yes
5	Prevent Use of # Previous Passwords	10	10	10	10	Last password cannot be used again.
6	Case Sensitive	Yes	Yes	Yes	Yes	Yes
7	Multi Factor	Not Required	Not Required	Not Required	Not Required	Yes
8	Privilege Access Management	Yes	Yes	Yes	No	No

Table 2: Password Settings

Bad password practices must be avoided. Passwords must not:

1. Include the User Logon ID.
2. Be a representation of frequently used words/passwords (e.g., P@ssw0rd, 123abc!).
3. Be shared with other users.

Specific policies and/or standards may supersede this standard when such policies / standards explicitly state that they supersede this standard. However, if the superseding policy/ standard does not address all the listed attributes, the default value be taken from the table above.

If multifactor authentication is required (e.g., use of token due to privacy concerns), the use of password can be replaced with an alternate authentication method.

4.3 Access Control Classification Framework

The minimum requirements for access control will vary based on the sensitivity, confidentiality and integrity of the data being protected. The confidentiality and integrity framework below guides the "Minimum Access Control Strength" required for each combination of "Confidentiality Level" and "Integrity Level." Within a single system, various roles within the system may require varying access control strength. Confidentiality and integrity levels are determined upon consultation with Corporate Information Management Services, who will assess the content of the information and classify it per the [Information Protection Classification Standard](#). Additionally, Office of the CISO may further be consulted for guidance as defined in the Access Management Policy section 9.1 Access Control and Credential Management Principles and Process Guiding Principle).

Sensitivity of information systems must be assessed, and the aggregate sensitivity rating of the information and assets involved must be documented.

Confidentiality is defined as preserving authorized restrictions on information access and disclosure. A loss of confidentiality is the unauthorized disclosure of information. Integrity is defined as guarding against improper addition, modification, or destruction of information. Enforcing integrity to preserve the timeliness, accuracy, and completeness of information.

4.3.1 Impact Ratings

Impact is measured according to the following four levels, Critical, High, Medium, and Low:

a. Critical

Inappropriate Access Control may:

- result in extensive cost or loss of major tangible assets or resources.

- extensively violate, harm, or impede an organization's mission, reputation, regulatory compliance, or interest.
- result in human deaths, serious or long-term injury, significant financial implications, or legal liability.

b. High

Inappropriate Access Control may:

- result in the highly costly loss of major tangible assets or resources.
- significantly violate, harm, or impede an organization's mission, reputation, or interest.

c. Medium

Inappropriate Access Control may:

- result in the costly loss of tangible assets or resources.
- violate, harm, or impede an organization's mission, reputation, or interest.

d. Low

Inappropriate Access Control may:

- result in the loss of some tangible assets or resources; or
- noticeably affect an organization's mission, reputation, or interest.

In the framework below, the required strength is dependent on the confidentiality level of the information the role can access and the integrity level of the information the role can add, delete, or modify. For example, if a role has access to High confidentiality information but can only add, modify, or delete Medium integrity information, the role must meet High Access Control Strength.

		Minimum Access Control Strength			
Integrity	High	High	High	High	High
	Medium	Medium	Medium	Medium	High
	Low	Low	Low	Medium	High
	Open (or Read-Only Access)	Negligible Control Required	Low	Medium	High
		Open	Low	Medium	High
Confidentiality Level					

Table 3: Access Control - Confidentiality and Integrity Framework

The table below describes the minimum access control requirements for various elements of access control. Choosing controls stronger than the minimum required is optional. The minimum access control requirements are based on the required level of access control strength from the table above.

Minimum Access Control Requirements Mapped to Various Elements of Access Control

Access Control Elements	Minimum Control Strength Low	Minimum Control Strength Medium	Minimum Control Strength High
Provisioning of Credentials	Pseudo-anonymous accounts are permitted. There is no requirement to positively identify the account holder.	<p>The identification process, account approval process and credential issuance process must be bound. This means that once a positive identification of the account requester is made, the results of the identification, along with the account request must be provided, to the Access Manager for approval. The approval notification must be sent by the Access Manager to the credential issuer who then issues the credential to the account requester.</p> <p>The provisioning process must be documented and validated.</p>	<p>The identification process, account approval process and credential issuance process must be bound. This means that once a positive identification of the account requester is made, the results of the identification, along with the account request must be provided to the Access Manager for approval. The approval notification must be sent by the Access Manager to the credential issuer who then issues the credential to the account requester.</p> <p>The provisioning process must be documented and validated.</p> <p>The minimum requirement for identification must be of equivalent validity to the City of Toronto's Human Resources identification process for employee on-boarding.</p>
Length of Time in which Temporary Authentication Credentials used for Initial Access will remain Valid if not used.	1 month	2 weeks	1 week
Maximum number of consecutive failed login attempts before account is locked out	10 times	5 times	4 times

Requirement for Positive User Identification before Authentication Credentials are Reset	No	Yes	Yes
Length of Time in which Temporary Authentication Credentials used for Password or “Something You Know” type Credential is Reset, will remain Valid if not used. (Recommended but not required) *	1 week*	1 day*	1 hour*
Transmitting Passwords or Other “Something You Know” type of credentials	User ID must be sent in a separate message from the message containing password. (e.g., separate email messages).	User ID must be sent in a separate physical communications channel from the password. (e.g. User ID by email and password by telephone).	Credentials must be transmitted encrypted.
Use of Generic User Accounts	Not Permitted	Not Permitted	Not Permitted
Authentication	Username and password at minimum must enforce the same password complexity as the City of Toronto’s corporate authentication service.	Username and password authenticated from a centralized authentication service (preferably City of Toronto’s corporate authentication service).	Enforces multi-factor authentication. Passwordless authentication should be considered to provide extra security assurance for cloud only Admin account.
Privilege Management	Role / privilege matrix documentation is not required.	Role / privilege matrix must be documented and validated against related business processes.	Business processes must be documented. Business process documentation must include roles and responsibilities. Role / privilege matrix must be documented and validated against related business processes documentation.
Activity Logging	Activity logs are optional.	The application should allow User ID and timestamp for all access to data to be recorded.	User ID and timestamp for all access to data must be recorded. Logs, or a copy of the logs must be

		Activity logs must be reviewed on a weekly basis.	recorded in a centralized log server. Activity logs must be reviewed daily.
Access Logs	User ID and timestamp of all successful and failed logon attempts should be recorded.	User ID and timestamp of all successful and failed logon attempts must be recorded. Access logs must be reviewed on a weekly basis.	User ID and timestamp of all successful and failed logon attempts must be recorded in a centralized log server. Access logs must be reviewed daily.
Periodic Access Control Review	Annual review.	Every six months.	Every three months.
Authentication to Cloud Services	May use service provider's authentication service.	Authentication controls must integrate with City of Toronto's central authentication service over a secure communications channel or from a secured device. Or must be as strict as City of Toronto authentication policies and require multi-factor authentication.	Must integrate with City of Toronto's central authentication service over a secure communications channel or from a secured device and Multi-factor authentication is required.
Cloud Service Provider must have logging and monitoring capability that allows isolation of an incident to specific clients	No	Yes	Yes
Cloud Service Provider must have identity management system which enables both role-based and context-based privilege management to data	No	Yes	Yes
Cloud Service Provider must provide City with multifactor authentication options for user	No	Yes (as per authentication to Cloud Services, see above)	Yes (as per authentication to Cloud Services, see above)

access (e.g., digital certificates, tokens, biometrics, etc.)			
Cloud Service Provider must utilize secure networks to provide management access to cloud service and multifactor authentication to admin function	No	Yes	Yes
Administrative access to Cloud Service Provider solution over the Internet must use multi-factor authentication	No	Yes (as per authentication to Cloud Services, see above)	Yes (as per authentication to Cloud Services, see above)

Table 4: Minimum Access Control Requirements Mapped to Various Elements of Access Control

4.4 Wireless Access

For Wireless Access, refer to the [Wireless Local Area Network Security Standard S130](#).

4.5 Remote Access

Secure remote access must be strictly controlled and authorized by City account owner or service provider. All hosts that are connected to City of Toronto's internal networks via remote access technologies must use the most up-to-date anti-virus software and OS patches.

Access control will be enforced via multifactor authentication (such as one-time password authentication or public/private keys with passphrases).

Employees and contractors with remote access rights must ensure that their personal device or device provided by the City of Toronto (e.g., workstation, tablet, smartphone) which is remotely connected to City of Toronto's corporate network, is not connected to any other network at the same time (i.e., split-tunnelling), with the exception of personal networks that are under the complete control of the user.

Personal equipment that is used to connect to City of Toronto's networks must meet the requirements of City of Toronto owned equipment for remote access.

Organizations or individuals who wish to implement non-standard Remote Access solutions to the City of Toronto production network must undergo a risk assessment and obtain prior approval by Technology Services Division and Office of the Chief Information Security Officer.

4.6 System Access Control

All vendor-supplied default User ID accounts (e.g., "Administrator" in Windows, "root" in Unix/Linux) shall be deleted, renamed, or disabled, and/or the passwords shall be altered before a system can be installed on the City of Toronto network. In addition, to detect inappropriate use of these IDs, logs of actual usage must be created and reconciled against authorized activities.

Vendor-supplied accounts that cannot be disabled or removed without also disabling the associated system, and where equivalent access rights cannot be granted to an ID assigned to an individual. In this case, every effort must be made to develop compensating controls to maintain individual accountability.

Authentication credentials must be stored separately from application data. Authentication credentials should be stored and processed within a centralized authentication system.

Authentication credentials must be stored and transmitted in a manner that ensures their confidentiality and integrity.

Storage of Service Account credentials must be compliant with Section 4.1.7 of the Cyber Credential Management Policy.

Passwords for Service Accounts in production systems must be different from their corresponding account in non-production systems.

4.6.1 System Use Notification

The information system displays an approved, system use notification message before granting system access. The notification informs potential users the following:

1. The user is accessing a City of Toronto information system.
2. System usage may be monitored, recorded, and subject to audit.
3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.
4. Use of the system indicates consent to monitoring and recording.

The system use notification message provides appropriate privacy and security notices (based on associated privacy and security policies or summaries) and remains on the screen until the user takes explicit actions to log on to the information system.

The system must not display passwords on the screen as they are being entered.

The system must validate the logon information only after all input data is entered. If an error condition is generated, the system must not indicate which part of the log-on data is correct or incorrect.

The information should notify the user, upon successful logon, of the date and time of the last logon.

4.6.2 Session Control

To prevent unauthorized access to the system, a session lock after 15 minutes of inactivity or upon receiving a request from a user must be initialized.

The session lock of a system (server or workstation) or application which prevents access to a subsystem or application should be considered a sufficient control for the subsystem or application to meet this requirement.

The information system session lock mechanism, when activated will hide what was previously visible on the screen.

A session lock:

1. Will be in effect until the user re-establishes access using established authentication procedures.
2. Is not a substitute for logging out of the information system.

4.6.3 Logging and Monitoring

All systems that make access control (authentication and authorization) decisions shall record and retain audit-logging information in accordance with [records management standards](#). Such logs must include:

1. The activity that was performed. Activity logs must not contain personal information or confidential business information.
2. Who or what performed the activity and where or on what system the activity was performed from (subject).
3. When the activity was performed.
4. What was the status (such as success vs. failure), outcome, or result of the activity.
5. Log all successful and unsuccessful log-on attempts.
6. Generate an alert if the maximum number of permitted unsuccessful logon attempts is reached.

4.7 Use of Information Systems by External Party

Accounts created by the City of Toronto to be used by third parties must:

1. Adhere to this standard.
2. First be requested and approved by the account owner's sponsor (equivalent to account owner manager) and the sponsor's manager (Business Division Head).

3. Complete a Risk Assessment conducted by the Office of the CISO, and risk accepted by the Business Division Head.
4. Be approved by the Office of the CISO.
5. Formally agree to abide by, and meet the City's technology, information and security policies and standards through a signed agreement prior to being granted access.

Accounts created for third parties for remote user access must be enabled only after being granted access by the system owner director (or equivalent) and disabled immediately after third party activities have been completed. All activities conducted by third parties must be logged, and their activities reviewed to ensure what was conducted was expected.

Accounts created to be used for external information system connections must have an associated City of Toronto sponsor that is accountable for provision/de-provision accounts as required.

Where relevant, or part of the risk assessment, third parties must be asked to provide a copy of their access controls policies/standard and if required, outline measures that they plan to take to ensure City's data and access to City's systems remain secure.

4.8 Use of Third-Party Systems

Connections to external third parties (e.g., information services providers, managed service providers, third-party cloud service providers, support providers,) to or from City of Toronto network must be, documented, limited to the minimum required to meet purpose of the connection and approved by the system owner.

Connections to external parties must be established only after the external party's information security and risk to the City has been assessed by the Office of the CISO and was found to be meeting with the City of Toronto information security requirements based on the accessed information and systems.

4.9 Use of Cloud Services

The use of cloud services must be assessed by the Office of the CISO to ensure the appropriate application of controls.

Related to access control:

- a) User credential/password must be securely stored using appropriate encryption/secure hash with proper salt.
- b) Cloud Service Provider must support open standard for identity management (e.g., SAML2, OpenID).
- c) Cloud Service Provider must establish un-alterable data audit trail (i.e., logs).

- d) Cloud Service Provider must have logging and monitoring capability that allows isolation of an incident to specific clients.
- e) Ensure Cloud Service Provider follow city policies related to access and credential management.

a. 4.10 User Responsibilities

4.10.1 Protecting Passwords

All users must review and sign-off on a password responsibility statement that is applicable to the system that they intend on using. All users, including contractors and vendors with access to City of Toronto systems, are responsible for taking the appropriate steps to select and secure their passwords. Do not use the "Remember Password" feature of applications (e.g., web browsers). Passwords must:

1. Not be shared with anyone, including administrative assistants, executive assistants, and managers, co-workers while on vacation, and family members.
2. Be treated as sensitive, confidential information.
3. Be transmitted securely as per Section 4.3 [Mapping of Access Control to Data Sensitivity Classification](#).
4. Not be revealed over the phone to anyone without properly validating the person's identity first, to ensure that the person is authorized to receive the information.
5. Not contain hints (e.g., "my family name").
6. Not be written down or stored anywhere in your office or in a file on a computer system or mobile devices (phone, tablet) without encryption.

Any user suspecting their password may have been compromised must report the incident to TSD Service Desk, the Office of the CISO, and their supervisor / manager. The potentially compromised password must immediately be changed. If the compromised credential is related to a privileged account or an account that has access to High confidentiality data or can modify High integrity data, the usage of the system by the compromised account must be reviewed to ensure that malicious activities did not occur.

4.10.2 Use of Access

City of Toronto users must never use their "Regular User" accounts to perform administrative tasks and regular accounts must not be granted administrator privileges. If required, a separate "Administrator Account" must be provisioned and required privileges granted to the account. This will ensure that the "minimum required privileges" principle is maintained, and that clear audit trail is created.

Only account owners, or their delegates, can provide access credentials to a "Generic User Account" – it is the account owner's responsibility to ensure the accessing user will not abuse the credentials.

4.10.3 Administrator Account Usage

Credentials of an Administrator Account must be protected more diligently than regular accounts (e.g., stronger password, frequent password changes – see Section 4.2 [Password Policy](#)). Users must properly logout from a system when using an Administrator Account and not wait for automatic logout/lockout. On prem and cloud admin accounts must be separated to limit the impact of compromise to other environments. Administrator accounts must:

1. Be used to conduct administrative tasks.
2. Not cache or store credentials for automated processes
3. Be such that even if a Regular account and an Administrator account is assigned to the same person, their authentication credentials (both UserID and secret credentials) must be different.
4. Only Local Administrator account may have local administrator rights to workstations and servers.
5. Never be used to perform regular user tasks (e.g., reading emails, composing documents). Their Administrator Account must enforce least privilege such that regular user tasks cannot be performed.
6. Have all their activities logged.
7. Not be shared with other users (even other administrators) as activities will be logged and associated with the account owner, if the account must be shared, it must be limited to the minimum required number of individuals.

If a user normally does not require administrative access to a system but is required to conduct a task, then the user may only be provided administrative access, after approval from the system owner, and only for the duration required to perform the task. Once the task is completed, the temporary Administrator access must be removed.

Generic administrator account must be avoided. If system limitations require the use of generic administrator accounts, then creation of a Generic Administrator account requires a risk assessment by the Office of the CISO and subsequent risk acceptance by the account owner before approval by the Office of the CISO (see link to Access Management Policy section 4.1.3).

5. Standard Approval and Review Schedule

The Technology Standards Technical Committee has developed this standard. The Committee members consist of technology and security representatives from City of Toronto Divisions, including the Technology Services Division. This Standard is submitted to the Enterprise Architecture Review Board for approval and is reviewed minimally every two years or as required.

6. Related Documents

- 6.1. [Access Management Policy \(002\)](#)
- 6.2. [Acceptable Use Policy \(1002\)](#)
- 6.3. [Cyber Security Policy \(001\)](#)
- 6.4. [Data Sensitivity Classification and Risk Guidelines](#)
- 6.5. [Elevated Account and Local Administrative Rights Request Form](#)
- 6.6. [Mobile Endpoint Device Security Standard \(S125\)](#)
- 6.7. [Wireless Local Area Network Security Standard \(S130\)](#)

7. Contact

Cloud and Internet Services

Email: Andrew.Chan@toronto.ca

APPENDIX A:

Roles & Responsibilities Matrix by Account Type

Legend:

Symbol	Name	Description
R	RESPONSIBLE	Ensures that the work is done, co-ordinates the work among those supporting, may also contribute to the work - There can be multiple "R" for each activity.
A	APPROVES	Signs off that the work was done (verifies quality and completion, concurs with the work) - Only one A per activity/deliverable.
S	SUPPORTS	Provides support and resources or does the work, if there is no "S" for a row, the "R" does the actual work.
C	CONSULTED	Must be consulted before activity/deliverable is completed; provides input/recommends solutions.
I	INFORMED	Must be informed of progress and/or the final results.
N/A	NOT APPLICABLE	Does not apply in this particular context.

Account Owner: This is the person who has been assigned the account. Credentials are associated to the account holder's identity.

Account Owner's Manager: Within the organizational structure, the Account Owner reports to this person.

Access Manager: Approves tasks related to access control.

Role Manager: This person is knowledgeable on which person should be assigned which role within a system.

System Administrator: Implements changes to the access control system.

Administrator Account

An account that has administrative or high privileges such as management of a system, services and/or application resources.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Disable Account (no longer required)	I	I	A	I	S
Periodic Review (Active and Disabled Accounts)	R	I	A	R	N/A
Owner moves within the organization (change role)	I	I	A	I	S
Owner Leaving/Termination	N/A	I	A	I	S

Regular User Account

An account that is used by City of Toronto user (staff or non-staff member) to access and operate City of Toronto systems. Such account is usually defined and is a part of the City of Toronto directory services.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Periodic Review (Active and Disabled Accounts)	R	I	A	R	N/A
Owner moves within the organization (change role)	I	C	A	I	S
Owner Leaving/Termination	N/A	I	A	I	S

Service Account

An account that is usually created to allow services and/or applications to interact with the operating system without user interface.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Disable Account (no longer required)	R	I	A	R	N/A
Periodic Review (Active and Disabled Accounts)	I	I	A	I	S
Owner moves within the organization (change role)	I	C	A	I	S
Owner Leaving/Termination	N/A	C	A	I	S

Generic User Account

An account that is used by multiple City of Toronto users.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Disable Account (no longer required)	R	I	A	R	N/A
Periodic Review (Active and Disabled Accounts)	I	I	A	I	S
Owner moves within the organization (change role)	I	C	A	I	S
Owner Leaving/Termination	N/A	C	A	I	S

Public Account

An account that is for users that are not related to City of Toronto, usually for public applications and/or services. Public account may be managed outside the City of Toronto directory services (e.g., local account repository managed by the application).

An account that has not been classified but has access to the City of Toronto internal network, will be defined and set as "Internal User" by default.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Periodic Review (Active and Disabled Accounts)	R	I	A	R	N/A
Owner Leaving/Termination	N/A	C	A	I	S

Cloud-Only Account

An account that is created and managed solely within City of Toronto Cloud environment (Azure/O365/AWS) to perform administration task and/or interact with operation system/API for user authentication.

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	I	C	A	I	S
Account Update (e.g., change permissions or policy)	I	C	A	I	S
Disable Account (no longer required)	I	I	A	I	S
Periodic Review (Active and Disabled Accounts)	R	I	A	R	N/A
Owner moves within the organization (change role)	I	I	A	I	S
Owner Leaving/Termination	N/A	I	A	I	S

Cloud Guest Account

An external account that is created or invited to City of Toronto Cloud environment (Azure/O365/AWS) for cloud resource collaboration.

Activity/Deliverable	ACCOUNT OWNER/City Sponsor	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Account Creation	R	C	A	I	S
Account Update (e.g., change permissions or policy)	R	C	A	I	S
Disable Account (no longer required)	I	I	A	I	S
Periodic Review (Active and Disabled Accounts)	R	I	A	R	N/A
Owner moves within the organization (change role)	R	I	A	I	S
Owner Leaving/Termination	R	I	A	I	S

Role Management

Activity/Deliverable	ACCOUNT OWNER	ACCOUNT OWNER'S MANAGER	ACCESS MANAGER	ROLE MANAGER	SYSTEM ADMINISTRATOR
Role Creation	I	N/A	A	R	S
Role Update (e.g., change permissions or policy)	C	N/A	A	R	S
Periodic Review (Active/Disabled Accounts within role)	N/A	N/A	A	R	N/A
Disable Role (no longer required)	I	N/A	A	R	S